Phishing Campaign Simulation Platform

Introduction

Phishing attacks represent one of the most prevalent cybersecurity threats faced by organizations today. To address this, simulated phishing campaigns are conducted to educate users, test organizational resilience, and enhance awareness. This project entails the creation of a secure and comprehensive platform that enables the simulation of realistic phishing campaigns for educational and training purposes.

Abstract

The project aimed to design and implement a web-based system allowing trainers to create, manage, and execute phishing simulation campaigns. Users can register, receive simulated phishing emails, and access educational content on email security. The solution enables tracking of user interactions, helping to identify vulnerabilities and provide targeted cybersecurity training.

Tools Used

- **Programming Language:** Python
- **Framework:** Flask (for web application routing and backend)
- **Frontend:** HTML/CSS (custom, for all forms and training modules)
- **Email Handling:** Python smtplib, email.mime
- **Database:** (Assumed) SQLite or similar (for user and campaign data)
- **Other Libraries:** Flask extensions (for forms, flashing messages)

Steps Involved in Building the Project

1. **Requirement Analysis:** Identified educational and campaign features.
2. **User Module Implementation:** Developed user registration and secure login workflow, with roles for trainees and trainers.
3. **Education Hub:** Built an integrated learning center with resources, best practices, and quizzes on identifying phishing.
4. **Email Template & Campaign System:** Enabled creation of customizable phishing email templates and bulk campaign setup, including user targeting.
5. **Email Sending Logic:** Wrote a Python emailing function with HTML tracking links, and integrated it into the campaign launch workflow.
6. **Result Tracking:** Incorporated mechanisms for tracking email opens and link clicks for user assessment.
7. **UI/UX:** Designed simple, clear web forms for all settings and actions to ensure usability for non-technical users.

Conclusion

This project provides a practical and interactive way to enhance cybersecurity awareness within organizations by safely simulating phishing attacks. The modular design allows easy updates for new phishing techniques and additional education features. Its scalable approach can be adapted for larger organizations, supporting continuous security training.